

CLAIMS

What is claimed is:

1 1. A method for a receiver to verify a security certificate for a sender comprising the
2 steps of:

3 receiving a first security certificate associated with the sender and storing the first
4 security certificate in a location accessible to the receiver;
5 updating the first security certificate in the location accessible to the receiver if the
6 first security certificate is changed or revoked;
7 receiving a second security certificate from the sender when identity of the sender
8 needs to be verified;
9 comparing the second security certificate to the first security certificate; and
10 confirming the sender's identity only if the second security certificate matches the
11 first security certificate for the sender.

1 2. The method of Claim 1, wherein the step of updating the first security certificate
2 comprises:

3 removing the first certificate from the location accessible to the receiver if the first
4 certificate is revoked; and
5 replacing the first certificate in the location accessible to the receiver if the first
6 certificate is changed.

1 3. The method of Claim 2, wherein the removing step is performed if the first certificate
2 is known to have been revoked for a reason selected from the group consisting of expiration
3 of the certificate, change of certificate authority, and compromise of the certificate.

- 1 4. The method of Claim 2, wherein the replacing step is performed if the first certificate
2 is known to have been changed for a reason selected from the group consisting of expiration
3 of the certificate, change of certificate authority, and compromise of the certificate.
- 1 5. The method of Claim 1, wherein the storing step comprises storing the first security
2 certificate in a directory service.
- 1 6. The method of Claim 5, wherein the directory service is a Lightweight Directory
2 Access Protocol directory.
- 1 7. The method of Claim 1, wherein the first certificate is known to have been granted by
2 a certificate authority.
- 1 8. The method of Claim 1, wherein the first certificate is known to have been obtained
2 in a trusted domain.
- 1 9. The method of Claim 1, wherein the step of comparing the first certificate and second
2 certificate comprises comparing a computer memory representation of each certificate.
- 1 10. The method of Claim 1, wherein the sender is a client and the receiver is a server.
- 1 11. The method of Claim 10, wherein the receiver is an authentication, authorization, and
2 accounting server.
- 1 12. The method of Claim 1, wherein the sender is a server and the receiver is a client.
- 1 13. The method of Claim 1, wherein the communication between the sender and receiver
2 is in a protocol that requires the inclusion of a digital certificate.

1 14. The method of Claim 13, wherein the protocol is selected from the group consisting
2 of the Extensible Authentication Protocol and Transport Level Security protocol, the
3 Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security
4 protocol.

1 15. The method of Claim 1, wherein the second certificate is known to have been signed
2 by a certificate authority.

1 16. The method of Claim 15, further comprising the step of decrypting the second
2 certificate using a public key associated with the certificate authority, whereby the receiver
3 verifies that the certificate authority has signed the second certificate.

1 17. The method of Claim 1, further comprising the step of validating that the sender has a
2 private key corresponding to a public key in the second certificate, this step comprising the
3 steps of:

4 receiving a message encrypted with the sender's private key; and
5 decrypting the message using the sender's public key.

1 18. A method for a server to verify a security certificate for a client comprising the steps
2 of:

3 copying a first security certificate associated with the client to a location accessible to
4 the server;
5 updating the first security certificate in the location accessible to the server if the first
6 certificate is changed or revoked;
7 receiving a second security certificate from the client when identity of the client
8 needs to be verified;
9 comparing the second security certificate to the first security certificate; and

10 confirming the client's identity only if the second security certificate matches the first
11 security certificate.

1 19. The method of Claim 18, wherein the step of updating the first certificate comprises:
2 removing the first certificate from the location accessible to the server if the first
3 certificate is revoked; and
4 replacing the first certificate in the location accessible to the server if the first
5 certificate is changed.

1 20. The method of Claim 19, wherein the removing step is performed if first certificate is
2 known to have been revoked for a reason selected from the group consisting of expiration of
3 the certificate, change of certificate authority, and compromise of the certificate.

1 21. The method of Claim 19, wherein the replacing step is performed if first certificate is
2 known to have been changed for a reason selected from the group consisting of expiration of
3 the certificate, change of certificate authority, and compromise of the certificate.

1 22. The method of Claim 18, wherein the location accessible to the server is a
2 Lightweight Directory Access Protocol directory.

1 23. The method of Claim 18, wherein the first certificate is known to have been granted
2 by a certificate authority.

1 24. The method of Claim 18, wherein the first certificate is known to have been obtained
2 in a trusted domain.

1 25. The method of Claim 18, wherein the server is an authentication, authorization, and
2 accounting server.

1 26. The method of Claim 18, wherein the step of comparing the first certificate and
2 second certificate comprises comparing a computer memory representation of each
3 certificate.

1 27. The method of Claim 18, wherein the communication between the client and server is
2 in a protocol that requires the inclusion of a digital certificate.

1 28. The method of Claim 27, wherein the protocol is selected from the group consisting
2 of the Extensible Authentication Protocol and Transport Level Security protocol, the
3 Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security
4 protocol.

1 29. The method of Claim 18, wherein the second certificate is known to have been signed
2 by a certificate authority.

1 30. The method of Claim 29, further comprising the step of decrypting the second
2 certificate using a public key associated with the certificate authority, whereby the server
3 verifies that the certificate authority has signed the second certificate.

1 31. The method of Claim 18, further comprising the step of validating that the client has a
2 private key corresponding to a public key in the second security certificate, this step
3 comprising the steps of:

4 receiving a message encrypted with the client's private key; and
5 decrypting the message using the client's public key.

1 32. A method for a client to verify a security certificate for a server comprising the steps
2 of:

3 receiving a first security certificate associated with the server and storing the first
4 security certificate in a location accessible to the client;

5 updating the first security certificate in the location accessible to the client if the first
6 security certificate is changed or revoked;
7 receiving a second security certificate from the server when identity of the server
8 needs to be verified;
9 comparing the second security certificate to the first security certificate; and
10 confirming the server's identity only if the second security certificate matches the
11 first security certificate for the server.

1 33. The method of Claim 32, wherein the step of updating the first certificate comprises:
2 removing the first certificate from the location accessible to the client if the first
3 certificate is revoked; and
4 replacing the first certificate in the location accessible to the client if the first
5 certificate is changed.

1 34. The method of Claim 33, wherein the removing step is performed if the first
2 certificate is known to have been revoked for a reason selected from the group consisting of
3 expiration of the certificate, change of certificate authority, and compromise of the
4 certificate.

1 35. The method of Claim 33, wherein the replacing step is performed if the first
2 certificate is known to have been changed for a reason selected from the group consisting of
3 expiration of the certificate, change of certificate authority, and compromise of the
4 certificate.

1 36. The method of Claim 32, wherein the step of comparing the two certificates
2 comprises comparing a computer memory representation of each certificate.

1 37. The method of Claim 32, wherein the server is an authentication, authorization, and
2 accounting server.

1 38. The method of Claim 32, wherein the communication between the client and server is
2 in a protocol that requires the inclusion of a digital certificate.

1 39. The method of Claim 38, wherein the protocol is selected from the group consisting
2 of the Extensible Authentication Protocol and Transport Level Security protocol, the
3 Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security
4 protocol.

1 40. The method of Claim 32, wherein the second certificate is known to have been signed
2 by a certificate authority.

1 41. The method of Claim 40, further comprising the step of decrypting the second
2 certificate using a public key associated with the certificate authority, whereby the client
3 verifies that the certificate authority has signed the second certificate.

1 42. The method of Claim 32, wherein the server is one of a plurality of load balanced
2 servers and each server of the plurality of load balanced servers has an identical security
3 certificate, whereby the client need not know to which of the plurality of servers it is
4 attached.

1 43. The method of Claim 32, further comprising the step of validating that the sender has
2 a private key corresponding to a public key in server's security certificate, this step
3 comprising the steps of:

4 receiving a message encrypted with the server's private key; and
5 decrypting the message using the server's public key.

1 44. A computer-readable medium carrying one or more sequences of instructions which,
2 when executed by one or more processors, causes the one or more processors to perform the
3 steps of:

4 receiving a first security certificate associated with the sender and storing the security
5 certificate in a location accessible to the receiver;
6 updating the first security certificate in the location accessible to the receiver if the
7 first security certificate is changed or revoked;
8 receiving a second security certificate from the sender when identity of the sender
9 needs to be verified;
10 comparing the second security certificate to the first security certificate; and
11 confirming the sender's identity only if the second security certificate matches the
12 first security certificate for the sender.

1 45. A system comprising:

2 a local area network; and
3 two or more devices communicatively coupled to the local area network; wherein one
4 or more of the devices are configured to perform the steps of:
5 receiving a first security certificate associated with the sender and storing the
6 security certificate in a location accessible to the receiver;
7 updating the first security certificate in the location accessible to the receiver
8 if the first security certificate is changed or revoked;
9 receiving a second security certificate from the sender when identity of the
10 sender needs to be verified;
11 comparing the second security certificate to the first security certificate; and
12 confirming the sender's identity only if the second security certificate matches
13 the first security certificate for the sender;

14 and one or more of the devices are configured to perform the steps of:
15 copying the first certificate to a location accessible to the sender;
16 updating the first certificate in the location accessible to the sender if the
17 certificate is changed or revoked; and
18 sending the first certificate to a receiver when the identity of the sender needs
19 to be verified.

1